

### **REMARKS**

The Office Action dated May 3, 2005 has been received and carefully noted. The following remarks are submitted as a full and complete response thereto. Claims 1, 9, and 10 have been amended, claim 8 has been cancelled, without prejudice or disclaimer, and claims 11-13 have been added. No new matter has been added, and no new issues are raised which require further consideration and/or search. Support for new claims 11-13 may be found, for instance, on page 5, lines 4-29, and page 6, lines 1-13.

Claims 1-7 and 9-13 stand rejected and pending and under consideration.

### **REJECTION UNDER 35 U.S.C. § 103:**

*In the Office Action, claims 1-10 were rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 6,305,423 to Hodges et al. ("Hodges") in view of U.S. Patent No. 6,192,237 to Clapton et al. ("Clapton"). The Office Action took the position that Hodges and Clapton disclose all the aspects of claims 1-10. The rejection is traversed and reconsideration is requested.*

Independent claim 1, upon which claims 2-9 are dependent, recites a method of updating a virus signature database used by anti-virus software operating on a mobile wireless platform, including sending update data via a signalling channel of a mobile telecommunications network to the mobile wireless platform, and sending virus update

Serial Number: 09/939,717

requests to the network server to identify to a network server updates required by the mobile wireless platform.

Independent claim 10 recites a method of protecting a wireless device against viruses including maintaining a database of virus signatures on the device, updating the database by receiving data containing virus signatures in one or more Short Message Service (SMS) or Unstructured Supplementary Services Data (USSD) messages, searching for virus signatures contained in the database, and sending virus update requests to the network server to identify to a network server updates required by the mobile wireless platform.

Independent claim 11, upon which claims 12-13 are dependent, recites a method for a mobile wireless platform includes sending a message from a mobile station to an anti-virus server, wherein the message indicates virus signatures stored in the mobile station. The method also includes in response to the message from the mobile station, generating concatenated return messages at the anti-virus server including virus signatures different from the virus signatures stored in the mobile station. The method sends the concatenated return messages from the anti-virus server to the mobile station to update the virus signatures stored in the mobile station.

As will be discussed below, the cited prior art of Hodges and Clapton fail to disclose or suggest the elements of any of the presently pending claims.

On page 2 of the Office Action, it is indicated that because “Hodges states ‘any of a

Serial Number: 09/939,717

variety of computer networking connection methods are also within the scope of the preferred embodiment' (column 6, lines 35-46), and further states that any connection can be used that 'assigns client computer an address for allowing the transmission of information to and from client computer' (column 6 lines 43-46). There is not a statement that limits the connection to TCP/IP connection as suggested by the applicant."

Applicants respectfully disagree with such assertion. Hodges is concerned with distributing virus signature files that contain signatures for all known viruses. Hodges repeatedly refers to ".DAT" files which are files containing all known signatures, which is an approach adopted by all anti-virus application vendors. See columns 7-8 of Hodges. The signature files are large, e.g., several hundreds of Kbytes or more. Although these files can be distributed easily over network connections such as those described in Hodges, a person of skill in the art would dismiss the possibility of sending such large files using the mechanism, i.e., USSD messages, of Clayton. USSD messages can carry a payload of only a few Kbytes. Even though USSD messages can be concatenated, to send a typical .DAT file would require the sending of several hundred USSD messages. As each message needs to be accepted by the recipient, this approach would not be practical.

The Applicants have been able to make the signalling channel approach work by "sending virus update requests to a network server to **identify** to the network server updates **required** by the mobile wireless platform" in a signature database (i.e. .DAT file) at the mobile terminal. Emphasis added. The volume of data involved in each update is relatively

small. However, based on the description provided in Hodges, a person of ordinary skill in the art can only conclude that when the update files are transmitted to a client computer 302, these update files also include virus signatures already stored in the client computer 302.

Furthermore, Hodges generally describes a method for updating local client computers with antivirus software updates from a central antivirus server. See column 4, lines 46-67. A desktop antivirus agent on client computer 302 generally remains dormant until the client computer 302 is connected to the Internet via a TCP/IP connection and an Internet interface program such as a Web browser is activated. See column 7, lines 20-27. According to Hodges, step 406 is a detection step, wherein the antivirus update agent queries the operating system of client computer 302 for an indication that a TCP/IP connection and that a Web browser has been invoked. At step 408 of Hodges, the antivirus update agent transmits a sequence of information packets to the central antivirus server 308 for notifying the central antivirus server 308 that a TCP/IP connection and a Web browser have been activated at client computer 302. See column 7, lines 28-39. Among the information transmitted from client computer 302 to central antivirus server 308 are two items of data used for achieving automated download and updating of antivirus files on client computer 302. In particular, (a) the IP address 305 of client computer 302 (e.g., 205.84.4.137), and (b) a unique user ID (e.g., "BJONES01234") are transmitted to central antivirus server 308.

However, Hodges fails to teach or suggest, "sending virus update requests to a network server to identify to the network server updates required by the mobile wireless

platform,” as recited in independent claims 1 and 10. Hodges is silent as to providing a virus update requests to the central antivirus server 308. Instead, Hodges indicates that the connection of the client computer 302 is what triggers the antivirus update agent in the client computer 302. Only when the connection of the client computer 302 is detected, the central antivirus server 308 receives the IP address 305 and the unique user ID. Also, only when the connection is established and the IP address 305 and the user ID are received will the central antivirus server 308 send the antivirus update files. Hodges does not provide that the client computer 302 identifies to the central antivirus server 308 the updates that are required by the wireless platform. Rather, as soon the connection is made by the client computer 302 and the identification is made by the central antivirus computer 302, the central antivirus computer 302 automatically sends update files. There is no transmission from the client computer 302 to the central antivirus server 308 of “virus update requests,” as recited in independent claims 1 and 10.

Referring to independent claim 11, Hodges describes that a client computer 302 remains dormant until the client computer 302 is connected to the Internet via a TCP/IP connection and an Internet interface program such as a Web browser is activated. See column 7, lines 20-30. The antivirus update agent queries the operating system of client computer 302 for an indication that a TCP/IP connection and that a Web browser has been invoked. Once the activation is detected, the client computer 302 transmits to a central antivirus server 308 an IP address 305 and a unique user ID. See column 7, lines 30-40. Once the activation

Serial Number: 09/939,717

is detected and the central antivirus server 308 identifies the client computer 302 using the IP address 305 and the unique user ID, the central antivirus server 308 automatically sends update files to the client computer 302. See column 7, lines 40-43.

However, Hodges fails to teach or suggest, “sending a message from a mobile station to an anti-virus server, wherein the message indicates virus signatures stored in the mobile station; in response to the message from the mobile station, generating concatenated return messages at the anti-virus server including virus signatures different from the virus signatures stored in the mobile station” as recited in independent claim 11. The client computer 302 of Hodges does not send a message to a central antivirus server 308 indicating the virus signatures already stored in the client computer 302. Although Hodges indicates that among information transmitted from the client computer 302 to the central antivirus server 308 are the IP address 305 and the unique user ID of the client computer 302, one cannot reasonably extend the information transmitted in Hodges to further include the virus signatures stored in the client computer 302 because Hodges is silent as to taking into consideration the virus signatures already included in the client computer 302. Based on the description provided in Hodges, a person of ordinary skill in the art can only conclude that when the update files are transmitted to the client computer 302, these update files also include virus signatures already stored in the client computer 302.

Hodges does not contemplate reducing the volume of information sent as part of a virus signature upgrade by “generating concatenated return messages” “in response to the

message from the mobile station,” as recited in independent claim 11. Hodges is silent as to providing concatenated return messages from the central antivirus server 308 to the client computer 302. Instead, Hodges indicates that the connection of the client computer 302 is what triggers the antivirus update agent in the client computer 302. Only when the connection of the client computer 302 is detected, the central antivirus server 308 receives the IP address 305 and the unique user ID. Also, only when the connection is established and the IP address 305 and the user ID are received will the central antivirus server 308 send the antivirus update files. There is no transmission from the client computer 302 to the central antivirus server 308 of a message indicating “virus signatures stored in the mobile station,” as recited in independent claim 11.

As correctly recognized in the Office action, there is no teaching or suggestion in Hodges of “sending update data via a signalling channel of a mobile telecommunications network to the mobile wireless platform,” as recited in independent claim 1, and “updating the database by receiving data containing virus signatures in one or more Short Message Service (SMS) or Unstructured Supplementary Services Data (USSD) messages,” as recited in independent claim 10. Accordingly, the Office Action relies on Clapton as describing such recitations.

In Clapton, an arrangement is provided allowing a user of a mobile telephone 11 to use intelligent network (IN) services specific to his home network. According to Clapton, when a user makes an outgoing call attempt, the associated signalling is transmitted over a

signalling channel (step 1). See column 5, lines 1-5. The user can be connected through an MSC 13 of a system other than his home system (a process known as “roaming”). However, Clapton does not cure the deficiencies of Hodges. Clapton does not relate to a method of updating a virus signature database used by anti-virus. Instead, Clapton limits its description to provide a call-set up process. Further, in Clapton, by merely indicating that outgoing calls from the user over the signalling channel, that alone does not teach or suggest, “sending update data via a signalling channel of a mobile telecommunications network to the mobile wireless platform,” as recited in independent claim 1.

Clapton limits its description to provide conventional uses of USSD messages. Specifically, Clapton provides that USSD has only been used to update more static customer data, such as setting up a call-forward arrangement representing advice of the user's own telephone number. See column 2, lines 51-57. However, there is no teaching or suggestion in Clapton of “updating the database by receiving data containing virus signatures in one or more Short Message Service (SMS) or Unstructured Supplementary Services Data (USSD) messages,” as recited in independent claim 10. Similarly, Applicants respectfully assert that Clapton is silent as to teaching or suggesting, at least, “in response to the message from the mobile station, generating concatenated return messages at the anti-virus server including virus signatures different from the virus signatures stored in the mobile station; and sending the concatenated return messages from the anti-virus server to the mobile station to update the virus signatures stored in the mobile station,” as recited in independent claim 11.

Serial Number: 09/939,717



There is nothing in Clapton to suggest that USSD messages may be used to carry application updates, such as anti-virus updates. Contrary to the contentions made in the Office Action, there is no teaching or suggestion in Clapton of providing any reference to SMS messages.

Accordingly, even if Hodges and Clapton were combined, a combination thereof would not provide for all the recitations of independent claims 1, 10, and 11. A combination of Hodges and Clapton would provide a client computer 302 sending a connection signal, a user ID, and an IP address to a central antivirus server 308 allowing a user of the client computer 302 to use intelligent network services specific to his home network, able to retrieve additional information from the user, such as a user service profile. However, a combination of Hodges and Clapton would be silent as to teaching or suggesting, at least, “sending virus update requests to a network server to identify to the network server updates required by the mobile wireless platform,” as recited in independent claims 1 and 10, and all of the recitations of independent claim 11.

It is respectfully requested that independent claims 1, 10, and 11 and related dependent claims be allowed.

## **CONCLUSION:**

In view of the above, applicant respectfully submits that the claimed invention recites subject matter which is neither disclosed nor suggested in the cited prior art. Applicants

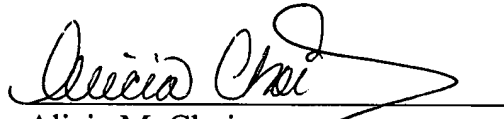
Serial Number: 09/939,717

further submit that the subject matter is more than sufficient to render the claimed invention unobvious to a person of skill in the art. Applicants therefore respectfully request that each of claims 1-7 and 9-13 be found allowable and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the Applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

  
Alicia M. Choi  
Registration No. 46,621 .

**Customer No. 32294**  
SQUIRE, SANDERS & DEMPSEY LLP  
14<sup>TH</sup> Floor  
8000 Towers Crescent Drive  
Tysons Corner, Virginia 22182-2700  
Telephone: 703-720-7856  
Fax: 703-720-7802

AMC:wmG

Serial Number: 09/939,717